CLAIMS

We claim:

1. A method comprising:

requesting a desired service through a foreign service provider;

generating a hash tree and generating a digital signature on a root value of the hash tree;

sending the digital signature and the root value to the foreign service provider;

providing one or more tokens to the foreign service provider with the next packet if the foreign service provider accepts the signature; and

continuing to use the service while the foreign service provider accepts tokens.

2. The method of Claim 1 further comprising a user device generating the one or more tokens.

3. The method of Claim 2 wherein the user device generates tokens using the hash tree.

4. The method of Claim 3 wherein the hash tree comprising a dense hash tree, and further comprising constructing the dense hash tree by:

randomly generating a number of bit streams equal to the number of tokens that is estimated to be needed;

constructing a binary tree with a number of leaves equal to the number of estimated tokens plus one;

assigning the random bit strings to the leaves; and

computing values to be assigned to each internal node according to the values of children of internal nodes.

5. The method defined in Claim 4 wherein generating a number of bit streams comprises generating the number of bits streams from a single seed.

6. The method of Claim 4 wherein the bit strings are of cryptographically suitable length.

7. The method of Claim 3 wherein the hash tree is one selected from a group consisting of a Merkle tree and a dense hash tree.

8. The method of Claim 1 wherein the user device generates the one or more tokens using a public key signature scheme, including using a public-key signature to sign the root of the hash tree.

9. The method of Claim 1 further comprising generating a digital signature on the root of the tree using a private signing key.

10. The method of Claim 1 wherein the user device includes in each of the one or more of the tokens one or more of a group consisting of the identity of the foreign service provider for which tokens are intended, a maximum number of tokens that the foreign service provider may receive, and any conditions that the foreign service provider must satisfy before it can redeem the token.

11. The method of Claim 1 further comprising sending to the foreign service provider a signature on the root value of the hash tree, a public key of the user device and a certificate from a trusted party attesting to a relationship between the user and their service provider.

12. The method of Claim 1 wherein the token is an undeniable token.

13. The method of Claim 1 comprising:

generating a dense hash tree;

providing the root value to a home service provider for signature;

informing the home service provider of the monetary value of the dense hash tree; and

providing payments based on the tree to the foreign service provider.

14. An apparatus comprising:

an external network interface through which a request for a desired service of a foreign service provider is made;

a memory;

a processor coupled to the external network interface and the memory, wherein the processor generates a hash tree and generates a digital signature on a root value of the hash tree using the memory, and further wherein the processor sends the digital signature and the root value to the foreign service provider, via the external network interface, along with one or more tokens with the next packet if the foreign service provider accepts the signature, and continues to use the service while the foreign service provider accepts tokens.

15. The apparatus of Claim 14 further comprising a user device generating the one or more tokens.

16. The apparatus of Claim 15 wherein the user device generates tokens using the hash tree.

17. The apparatus of Claim 16 wherein the hash tree is one selected from a group consisting of a Merkle tree and a dense hash tree.

18. The apparatus of Claim 14 wherein the processor generates the one or more tokens using a public key signature scheme, including using a public-key signature to sign the root of the hash tree.

19. The apparatus of Claim 14 wherein the processor includes in each of the one or more of the tokens one or more of a group consisting of the identity

of the foreign service provider for which tokens are intended, a maximum number of tokens that the foreign service provider may receive, and any conditions that the foreign service provider must satisfy before it can redeem the token.

20. The apparatus of Claim 14 wherein the processor causes a signature on the root value of the hash tree, a public key of the user device and a certificate from a trusted party attesting to a relationship between the user and their service provider to the foreign service provider via the external network interface.

21. The apparatus of Claim 14 wherein the token is an undeniable token.

22. The apparatus of Claim 14 wherein the processor provides a root value of a dense hash tree to a home service provider for signature and informs the home service provider of the monetary value of the dense hash tree to enable the home service provider to pay the foreign service provider for the service.

23. An apparatus comprising:

means for requesting a desired service through a foreign service provider;

means for generating a hash tree and generating a digital signature on a root value of the hash tree;

means for sending the digital signature and the root value to the foreign service provider;

means for providing one or more tokens to the foreign service provider with the next packet if the foreign service provider accepts the signature; and

means for continuing to use the service while the foreign service provider accepts tokens.

24. An article of manufacture having one or more recordable media storing instructions thereon which, when executed by a system, cause the system to perform a method comprising:

requesting a desired service through a foreign service provider;

generating a hash tree and generating a digital signature on a root value of the hash tree;

sending the digital signature and the root value to the foreign service provider;

providing one or more tokens to the foreign service provider with the next packet if the foreign service provider accepts the signature; and

continuing to use the service while the foreign service provider accepts tokens.

25. A method comprising:

receiving a service request for a service from a user having a different service provider than the service provider providing the service;

receiving a digital signature, a root value and a certificate from the user; and

providing a service to the user in response to determining that the signature is acceptable and receiving one or more tokens from the user.

26. The method of Claim 25 further comprising verifying the signature from the user using a verification algorithm.

27. The method of Claim 26 wherein the verification algorithm outputs a Boolean value indicating whether the signature is valid based on the signature, a public key and a message.

28. The method of Claim 25 wherein the one ore more tokens include a hash pre-dash image.

29. The method of Claim 25 further comprising providing service after the token is received.

30. The method of Claim 25 further comprising providing service prior to receiving the token.

31. The method of Claim 25 further comprising providing service incrementally in conjunction with receiving a plurality of tokens.

32. The method of Claim 25 wherein the token is an undeniable token.

33. The method of Claim 25 further comprising a transmitting the one or more tokens to a home service provider of the user with the user's signature as well as information that was signed.

34. The method of Claim 33 wherein the information that was signed comprises the root value of a hash tree.

35. The method of Claim 25 further comprising verifying a portion of the tokens received and adjusting the polling based on prior user undesirable activity with respect to the validity of the tokens.

36. A foreign service provider comprising:

an external network interface through which a request for a desired service is received from a user device having a different service provider than the service provider providing the service, along with a digital signature, a root value and a certificate from the user device;

a memory to store program instructions;

a processor coupled to the external network interface and the memory, wherein execution of the program instructions causes the processor to determine if the signature is acceptable, to receive the one or more tokens, and to provide a service to the user device in response to determining that the signature is acceptable and receiving one or more tokens from the user device.

37. The foreign service provider of Claim 36 wherein the processor verifies the signature from the user using a verification algorithm.

38. The foreign service provider of Claim 36 wherein the one ore more tokens include a pre-hash image.

39. The foreign service provider of Claim 36 wherein the token is an undeniable token.

40. The foreign service provider of Claim 36 wherein the processor, via the network interface, transmits the one or more tokens to a home service provider of the user with the user's signature as well as information that was signed.

41. An apparatus comprising:

means for receiving a service request for a service from a user having a different service provider than the service provider providing the service;

means for receiving a digital signature, a root value and a certificate from the user; and

means for providing a service to the user in response to determining that the signature is acceptable and receiving one or more tokens from the user.

42. An article of manufacture having one or more recordable media storing instructions thereon which, when executed by a system, cause the system to perform a method comprising:

receiving a service request for a service from a user having a different service provider than the service provider providing the service;

receiving a digital signature, a root value and a certificate from the user; and

providing a service to the user in response to determining that the signature is acceptable and receiving one or more tokens from the user.

43. A method comprising:

receiving a user token from a service provider that is different from the service provider of the user;

determining if the token is valid; and

charging the user based on the token if the token is valid.

44. The method of Claim 43 further comprising following a dispute resolution policy if the token is not valid.

45. A home service provider comprising:

an external network interface through which a user token is received from a service provider that is different from the service provider of the user;

a memory to store program instructions;

a processor, coupled to the external network interface and the memory, to execute the program instructions to determine if the token is valid and to cause the user to be charged based on the token if the token is valid.

46. The home service provider of Claim 45 wherein the processor follows a dispute resolution policy if the token is not valid.

47. An apparatus comprising:

means for receiving a user token from a service provider that is different from the service provider of the user;

means for determining if the token is valid; and

means for charging the user based on the token if the token is valid.

48. The apparatus of Claim 47 further comprising means for following a dispute resolution policy if the token is not valid.

49. An article of manufacture having one or more recordable media storing instructions thereon which, when executed by a system, cause the system to perform a method comprising:

receiving a user token from a service provider that is different from the service provider of the user;

determining if the token is valid; and

charging the user based on the token if the token is valid.

50. The article of manufacture of Claim 49 wherein the method further comprises following a dispute resolution policy if the token is not valid.

51. A method comprising:

determining a number of packets that are to be transmitted;

generating a binary tree having a number of leaves equal to the number of packets;

assigning a random value to each leaf on the binary tree;

assigning, to each internal node, a value to be the output of the hash of the concatenation of values of children; and

assigning numbers to nodes that are the all left children in relation to the root.

52. An apparatus comprising:

an external network interface through which a request for a desired service of a foreign service provider is made;

a memory to store program instructions;

a processor coupled to the external network interface and the memory, wherein the processor executes the program instructions to determine a number of packets that are to be transmitted, generate a binary tree having a number of leaves equal to the number of packets, assigns a random value to each leaf on the binary tree, assign, to each internal node, a value to be the output of the hash of the concatenation of values of children, and assigs numbers to nodes that are the all left children in relation to the root.

53. An apparatus comprising:

means for determining a number of packets that are to be transmitted;

means for generating a binary tree having a number of leaves equal to the number of packets;

means for assigning a random value to each leaf on the binary tree;

means for assigning, to each internal node, a value to be the output of the hash of the concatenation of values of children; and

means for assigning numbers to nodes that are the all left children in relation to the root.

54. An article of manufacture having one or more recordable media storing instructions thereon which, when executed by a system, cause the system to perform a method comprising:

determining a number of packets that are to be transmitted;

generating a binary tree having a number of leaves equal to the number of packets;

assigning a random value to each leaf on the binary tree;

assigning, to each internal node, a value to be the output of the hash of the concatenation of values of children; and

assigning numbers to nodes that are the all left children in relation to the root.